## Ein revolutionäres Konzept

Es ist der 31.10.2008, als eine Gruppe Kryptografieinteressierter eine E-Mail erhält. Unterzeichnet ist diese E-Mail von Satoshi Nakamoto – ein bis zu diesem Zeitpunkt vollkommen unbekannter Name, der später als Erfinder des Bitcoins und Erzeuger des Genesis-Blocks in die Geschichte eingehen wird. Nakamoto berichtet über ein neues elektronisches Zahlungssystem, das vollständig auf einem dezentralen System beruht und keine Moderation seitens eines vertrauenswürdigen Dritten erfordert. Mithilfe von Bitcoin, wie Nakamoto seine Währung nennt, soll es von nun an möglich sein, den Transfer einer Währungseinheit direkt von Computer zu Computer, von einer Person zur nächsten zu ermöglichen. Die Anwendung gleicht den Eigenschaften von Bargeld, nur eben in digitaler Form. [...] In Presseberichten über Bitcoin findet man in der Regel Geschichten über das halsbrecherische Auf und Ab der Kryptowährung, über das Darknet, in dem mit Bitcoins bezahlt wird, oder von der bis heute erfolglosen Suche nach Satoshi Nakamoto, dem Erfinder von Bitcoin. Nur selten liest man über Bitcoin als ein epochales Konzept, das einen grundlegenden Wandel des heutigen Bankwesens herbeiführen könnte.

Rosenberger, P. (2018). Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Springer: Berlin, S. 1 und S. 9.

## Kontrolle in einem dezentralen System mit Hilfe der Blockchain.

Wie können in einem dezentralen System die Besitzansprüche an einer digitalen Münze eindeutig geklärt werden und wie kann sichergestellt werden, dass es diese Münze nur einmal gibt und sie nicht doppelt ausgegeben werden kann? Das Fehlen einer zentralen Instanz macht es schwierig, hier die Kontrolle zu behalten, denn theoretisch könnte in einem dezentralen System dieselbe Münze an unterschiedlichen Stellen gleichzeitig erzeugt werden. Um dies zu verhindern und gleichzeitig die Historie sämtlicher Transaktionen von Bitcoins zu verwalten, hat Nakamoto die Blockchain erfunden. Die Blockchain ist im Grunde eine endlose Liste aller Blöcke, die wiederum einzelne, bestätigte Transaktionen bündeln [...]. Jeder Block, der neu erzeugt wird, wird dieser Liste hinzugefügt. Die Bitcoin-Blockchain enthält somit Einträge sämtlicher jemals getätigter Transaktionen. Über entsprechende Online-Plattformen wie blockchain.info ist die Blockchain für jedermann einsehbar, unabhängig davon, ob er die Bitcoin-Software installiert hat oder nicht. Wer die Transaktion namentlich vorgenommen hat, kann der Blockchain jedoch nicht entnommen werden. Bitcoin ist somit transparent und nahezu anonym. [...] In der Blockchain werden sämtliche Transaktionen in chronologisch geordneten Blöcken registriert und schlussendlich verifiziert. Ist die Verifizierung erfolgreich, erzeugt das System den nächsten Block und verkettet ihn mit dem zuvor als gültig anerkannten Block. [...] Somit ist es nicht möglich, eine der digitalen Münzen doppelt auszugeben. Das Fälschen der Kryptowährung Bitcoin ist somit faktisch nicht möglich.

Rosenberger, P. (2018). Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Springer: Berlin, S. 18 f.

## Wie entstehen Bitcoins?

In dem Moment, in dem eine Transaktion, also eine Bitcoin-Überweisung, von A nach B transferiert wird, verschickt die Software, die der Nutzer verwendet, die Transaktion im Hintergrund an alle Nodes, die der Software zu diesem Zeitpunkt bekannt sind. Die sogenannten Nodes sind die Knotenpunkte des Netzwerks. Sie überprüfen und verifizieren die Transaktion, in der unter anderem die Bitcoin-Adresse des Versenders, die des Empfängers und natürlich die Höhe des zu versendenden Betrags hinterlegt sind, und senden sie anschließend an alle Nodes, die wiederum ihnen bekannt sind bzw. mit denen sie zu diesem Zeitpunkt verknüpft sind. Auf diese Art breitet sich die Transaktion nach und nach über das gesamte Bitcoin-Netzwerk aus, bis sie schlussendlich allen Nodes des Netzwerks bekannt ist. An dieser Stelle kommen die Miner ins Spiel. Sie sind für die Überwachung der Transaktionen und deren Einmaligkeit zuständig. Ihre Aufgabe besteht darin, aus vielen Transaktionen einzelne Blöcke zu generieren und diese der Blockchain hinzuzufügen. Dieser Vorgang ist [...] sehr rechenintensiv und verlangt nach spezieller Hardware und jeder Menge Strom. Nur durchschnittlich alle zehn Minuten wird eine dieser komplexen Berechnungen im Netzwerk gelöst. Ein neuer Block wird erst dann in die Blockchain, das Bitcoin-Grundbuch, geschrieben, wenn er von einer definierten Menge anderer Miner überprüft wurde. Der erzeugte Block macht die Versuche der übrigen Miner dadurch hinfällig. Sie übernehmen die Daten des neu erzeugten Blocks. Im Gegenzug erhält der Miner, der einen gültigen Block erzeugt und der Blockchain hinzufügt, als Belohnung die geschöpften Bitcoins und Gebühren aus den im Block enthaltenen Transaktionen. [...] Nach dem Hinzufügen des Blocks wird die aktualisierte Blockchain über das Netzwerk verbreitet und dort wiederum von den Nodes auf Gültigkeit überprüft. [...]

Rosenberger, P. (2018). Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Springer: Berlin, S. 19 f.